WHAT IS CLAIMED IS:

1. A method to verify authenticity of a document having an electronic signature associated therewith, said document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, the method comprising the following steps:

(a) creating a document identification number (DID) uniquely associated with said DFP, and associating said DID with said DFP;

(b) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP; and

(c) storing, in at least one location, registration certificate information (DFC) that represents said electronic signature and includes said DID, said DFP, and said C, such that a single entity cannot modify every stored copy of said DFC;

wherein authenticating whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

comparing a putative digital fingerprint DPF' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with the DFC stored at step (c);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

2. The method of claim 1, wherein at step (b), said credential information (C) is obtained from a user-registrant who initiates said association of said DID with said DFP.

3. The method of claim 1, wherein at step (a), said credential information (C) includes at least one type of information selected from a group consisting of (i) user-registrant identity, (ii) user-registrant password, (iii) user-registrant provided authenticating information from a two-factor authentication device, (iv) user-registrant cryptographic key information, (v) user-registrant client system identifier, and (vi) user-registrant provided authenticating hardware token information.

4. The method of claim 1, wherein at step (a), said association of said DID with said DFP is initiated by a user-registrant, said user-registrant selecting an archive-server in which said DF and at least DFC information will be stored.

5. The method of claim 1, further including storing said DF and at least DFC information in an archive-server, said archive-server verifying authenticity of said DF and said at least DFC information stored therein.

6. The method of claim 1, wherein step (a) includes selecting a document identification number (DID) at least quasi-randomly.

7. The method of claim 1, wherein step (a) includes generating said document identification number (DID) by a nexus-server.

8. The method of claim 1, wherein said DFP is representable in at least one format selected from a group consisting of (i) a printable bar-code, (ii) a printable multi-dimensional bar-code, (iii) printed scannable information, (iv) scannable information, and (v) human-readable information.

9. The method of claim 1, wherein step (c) includes selecting locations for said storage at least quasi-randomly.

10. The method of claim 1, wherein said document is protectable by copyright law, and said method is carried out at least in part to protect a copyright for said document, wherein said copyright law is selected from a group consisting of (i) U.S. copyright law, and (ii) copyright law of nations other than the U.S..

11. The method of claim 1, wherein step (c) includes initially promulgating said DFC to at least a minimum number Q of N, where $N \geq Q$, storage locations (WS), and subsequently promulgating said DFP to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC.

12. The method of claim 11, wherein step (c) includes initially promulgating said DFC substantially in real-time.

13. The method of claim 11, wherein:

each of said Q storage locations independently determines and independently reports a timestamp including time of its receipt of said DFP; and

said DFC stored at step (c) includes at least each independently reported said timestamp.

14. The method of claim 13, further including:

comparing time reported from each said timestamp to determine from a commonality thereof that time at which storing at step (c) occurred is not disputable.

15. A method to verify authenticity of a document having an electronic signature associated therewith, said document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, the method comprising the following steps:

(a) creating a document identification number (DID) uniquely associated with said DFP, and associating said DID with said DFP;

(b) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP;

(c) creating a signature declaration (SD) that captures expressed intent of a user-registrant to create and associate said electronic signature with said document represented by said DF;

(d) creating a testimonial record (T) that includes at least said DID, said DFP, said C, and said SD, and creating from and associating with said T a unique digital fingerprint number (DFP_T), said DFP_T obtainable from a cryptographic hash function (CHF_T); and

(e) storing, in at least one location, registration certificate information (DFC_T) that represents said electronic signature and includes said DID, said DFP, said DFP_T, and said C, such that a single entity cannot modify every stored copy of said DFC_T;

wherein authenticating whether a putative document, digitally representable as a putative file DF' and associated with a putative registration certificate (DFC_T') and associated with a putative testimonial record (T'), is an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

comparing a putative digital fingerprint DFP' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with the DFC_T stored at step (e), and

comparing a putative digital fingerprint DFP_T' for said T' obtained using said CHF_T with at least one copy of said DFP_T associated with the DFC_T stored at step (e);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and if said DFP_T ' and said DFP_T are in agreement, said electronic signature has not been altered.

16. The method of claim 15, wherein said DF includes a DFC_T previously stored at step (e).

17. The method of claim 15, further returning to said user-registrant information that includes at least said T and said DFP_T.

18. The method of claim 15, further including storing within a system-of-record information that includes at least said T.

19. The method of claim 15, wherein step (b) is carried out by a system-of-record that stores information including at least said T.

20. The method of claim 15, wherein at step (b), said credential information (C) is obtained from a user-registrant who initiates said association of said DID with said DFP.

21. The method of claim 15, wherein at step (b), said credential information (C) includes at least one type of information selected from a group consisting of (i) user-

registrant identity, (ii) user-registrant password, (iii) user-registrant two-factor authentication, and (iv) user-registrant key information.

22. The method of claim 15, wherein at step (a), said association of said DID with said DFP is initiated by a user-registrant, said user-registrant selecting an archive-server in which said DF and at least DFC information will be stored.

23. The method of claim 15, further including storing said DF and at least DFC information in an archive-server, said archive-server verifying authenticity of said DF and said at least DFC information stored therein.

24. The method of claim 15, wherein step (a) includes selecting a document identification number (DID) at least quasi-randomly.

25. The method of claim 15, wherein step (a) includes generating said document identification number (DID) by a nexus-server.

26. The method of claim 15, wherein step (e) includes selecting locations for said storage at least quasi-randomly.

27. The method of claim 15, wherein step (e) includes initially promulgating said DFC to at least a minimum number Q of N, where $N \geq Q$, storage locations (WS), and subsequently promulgating said DFP to any remaining (N-Q) said storage locations not initially receiving promulgated said DFC.

28. The method of claim 27, wherein step (e) includes initially promulgating said DFC substantially in real-time.

29. The method of claim 27, wherein:

each of said Q storage locations independently determines and independently reports a timestamp including time of its receipt of said DFP; and

said DFC stored at step (e) includes at least each independently reported said timestamp.

30. The method of claim 29, further including:

comparing time reported from each said timestamp to determine from a commonality thereof that time at which storing at step (c) occurred is not disputable.

31. A method to verify authenticity of a document optionally having an electronic signature associated therewith, said document being digitally representable as a file (DF) processable with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, where (i) a document identification number (DID) uniquely associated with said DFP has been created and associated with said DFP; where (ii) credential information (C) has been obtained, its veracity confirmed, and said C associated with said DID and said DFP; and (iii) where there has been stored in at least one location registration certificate information (DFC) representing said electronic signature and including said DID, said DFP, and said C, such that a single entity cannot modify every stored copy of said DFC; the method comprising the following steps:

(a) for a putative document, obtaining a digital representation thereof as a putative file DF' and obtaining a putative registration certificate (DFC') associated therewith;

(b) obtaining and comparing a putative digital fingerprint DPF' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with said DFC;

wherein said putative document is an unaltered version of said document represented by said DF and is associated with said electronic signature; and includes:

if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

32. A method to authenticate the identity of a user-registrant, the method comprising the following steps:

(a) selecting information at least identifying said user-registrant;

(b) using secret information known only to and provided by said user-registrant to cryptographically encode said information selected at step (a), without which secret information decoding of information encoded at step (b) cannot be accomplished;

(c) representing information cryptographically encoded at step (b) as a digitally encoded record (DER), and associating said DER with a document under control of said user-registrant;

wherein if an entity wishes to authenticate its identity as the user-registrant controlling said document with which said DER has been associated at step (c), said entity decodes information encoded at step (b).

33. A system to verify authenticity of a document representable digitally, the system comprising:

a nexus-server having a CPU and memory and including means for quasi-randomly generating ID numbers, issuing customer ID numbers, issuing document ID numbers (DID), and issuing coupons bearing at least one of (i) CID, and (ii) DID;

at least one cluster of witness-server computer systems (WS), each having a CPU and memory, each of said witness-servers being operatively coupleable to each other and to said nexus-server for intercommunication therebetween;

wherein said nexus-server supervises adherence of said WS in a cluster to rules and protocols applicable to said cluster;

wherein at least one of said WS, upon presentation by a user of said coupon and a digital fingerprint number (DFP) for said document obtained from a one-way cryptographic hash function (CHF), promulgates said coupon information and said DFP to at least a minimum number of other of said witness-server computer systems in said cluster, and upon confirming receipt of said coupon information and said DFP from said minimum number, said one of said witness-server computer systems converting said coupon into a registration certificate containing at least said coupon information and said DFP, said registration certificate is returned to said user;

said system upon user-presentation of said registration certificate retrieving from at least some of said witness-server computer systems in said cluster a digital fingerprint number;

wherein comparison of the retrieved said digital fingerprint numbers against a digital fingerprint number newly generated for said document permits confirming said document has was not altered after presentation to said system.

34. Media storing computer-readable software that when executed by a computer system that includes a CPU carries out at least three of the following steps to verify authenticity of a document having an electronic signature associated therewith, the document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF:

(a) obtaining and authenticating veracity of credential information (C), and associating said C with said DID and said DFP;

(b) creating a signature declaration (SD) capturing expressed intent of a user-registrant to create and associate said electronic signature with said document;

(c) promulgating for storage, in at least one location, registration certificate information (DFC) that represents said electronic signature and includes said DID, said DFP, said C, and at least one of (i) said SD, and (ii) a digital fingerprint of said SD, such that a single entity cannot modify every stored copy of said DFC;

wherein authenticating whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is an unaltered version of said document represented by said DF and is associated with said electronic signature includes:

(d) comparing a putative digital fingerprint DPF' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with the DFC stored at step (c);

wherein if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered.

35. For use with a system that can verify authenticity of a document having an electronic signature associated therewith, the document being digitally representable

as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, where said system (a) obtains and authenticates veracity of credential information (C), and associating said C with said DID and said DFP; (b) creates a signature declaration (SD) capturing expressed intent of a user-registrant to create and associates said electronic signature with said document; and (c) promulgates for storage registration certificate information (DFC) representing said electronic signature and including said DID, said DFP, said C, and at least one of (i) said SD, and (ii) a digital fingerprint of said SD, said system able to authenticate whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is an unaltered version of said document represented by said DF and is associated with said electronic signature by (d) comparing a putative digital fingerprint DPF' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with the DFC stored at step (c) such that if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered;

computer-readable medium storing at least one of said DID and said DFP.

36. A coupon dispenser for use with a system that can verify authenticity of a document having an electronic signature associated therewith, the document being digitally representable as a file (DF) that is processed with a cryptographic hash function (CHF) to yield a unique digital fingerprint number (DFP) associated with said DF, where said system (a) obtains and authenticates veracity of credential information (C), and associating said C with said DID and said DFP; (b) creates a signature declaration (SD) capturing expressed intent of a user-registrant to create and associates said electronic signature with said document; and (c) promulgates for storage registration certificate information (DFC) representing said electronic signature and including said DID, said DFP, said C, and at least one of (i) said SD, and (ii) a digital fingerprint of said SD, said system able to authenticate whether a putative document digitally representable as a putative file DF' and by a putative registration certificate (DFC') associated therewith is an unaltered version of said document represented by said DF and is associated with said electronic signature by (d) comparing a putative digital fingerprint DPF' for said DF' obtained using said CHF with at least one retrieved copy of said DFP associated with

the DFC stored at step (c) such that if said DFP' and said DFP are in agreement, said putative document is said document, and said electronic signature has not been altered; said coupon including at least said DID.